



*TOMORROW
starts here.*

Cisco *live!*



Advanced Email Security with ESA

BRKSEC – 3770

Joe Montes

Consulting Systems Engineer - Security

#clmel

Cisco *live!*

Agenda

- Introduction to Phishing
- Message Authentication
 - SPF
 - DKIM
 - DMARC
- Enhanced Security Features
- Q & A



Abstract

Phishing is the plague of today's e-mail communication. With modern anti-spam rendering legacy spam almost non-existent, different variants of phishing attacks are becoming the primary threat to global e-mail systems. Several authentication methods have been around for a while, but their adoption was low and not properly encouraged, and they mostly solved just parts of the problem. However, recent developments upgrade on those legacy techniques, and make message authentication, reporting and visibility part of Internet standards.

This advanced session will provide an in-depth review of SPF, DKIM and DMARC, the prevalent message authentication techniques, and how Cisco E-mail Security products can utilise them.

We will architect a real-world message authentication architecture and show through examples how, once implemented by all parties, it makes phishing with your identity impossible. Proper implementation of e-mail authentication techniques not only prevents you from being phished, but also helps protect your identity and brand reputation, and keeps you a reliable, trustworthy communication and business partner.



Introduction to Phishing

What is Phishing?

“**phish-ing** *noun* \ 'fi-shiŋ \

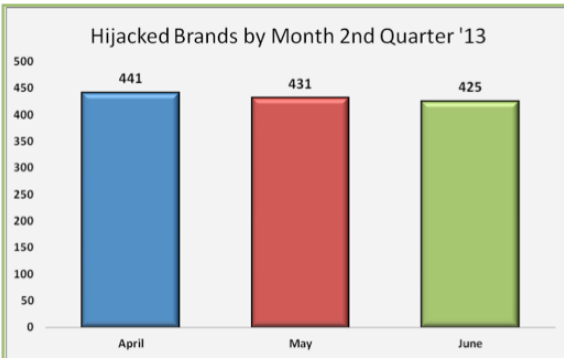
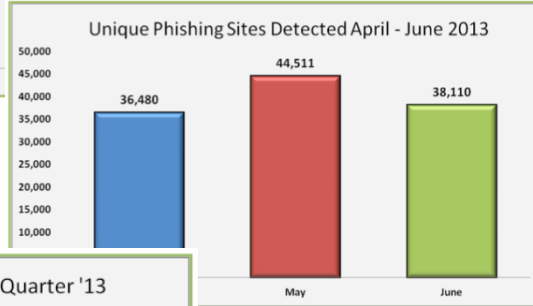
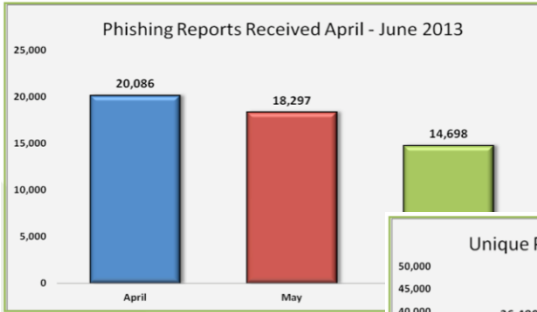
a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly”

- Merriam-Webster Online Dictionary

A Short History of Phishing

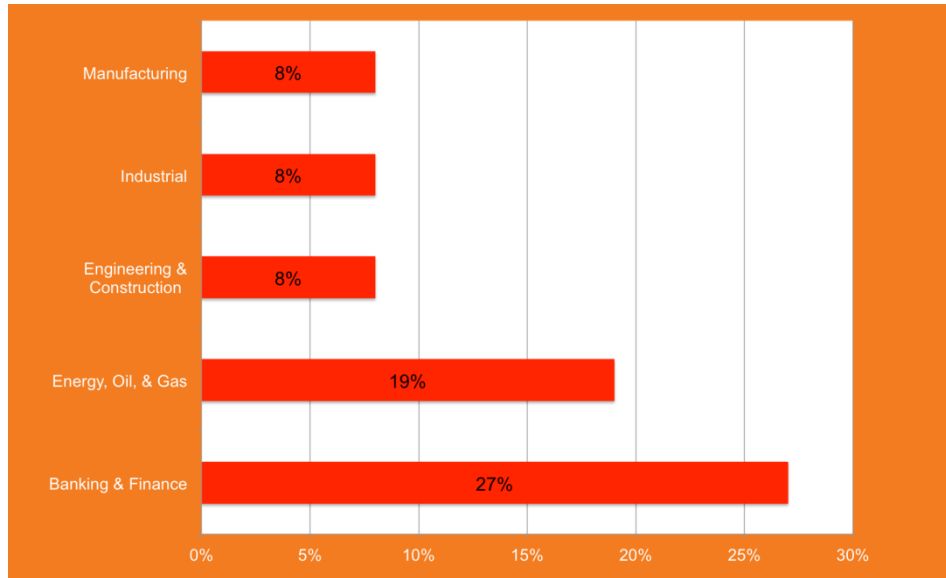
- First use: 1996, alt.online-service.america-online
- 2001
 - Moved to wider Internet, targeting payment systems
 - Easy to spot messages, spelling errors...
- 2003
 - Legitimate site opens in the background, phisher runs a fake login window in front.
 - Gartner reports global cost of phishing in 2003 at 2.4 billion US\$.
- 2004
 - Implemented data validation with real sites
 - Creating completely fake Websites of imaginary banks and financial firms.

Phishing Today



- Country hosting most target sites: USA
- Top 5 countries by attacked brands: USA, UK, India, Australia, France
- Most phishing attacks are launched on Fridays
- **Worldwide cost of Phishing in 2013: >5.9 billion US\$**

Who Is Attacked?



Source: Cisco TRAC Q1 2014 Quarterly Threat Briefing

- Energy sector targets in Q1:
 - An oil and gas exploration firm with operations in Africa, Morocco, and Brazil;
 - A company that owns multiple hydro electric plants throughout the Czech Republic and Bulgaria;
 - A natural gas power station in the UK;
 - A gas distributor located in France;
 - An industrial supplier to the energy, nuclear and aerospace industries;
 - Various investment and capital firms that specialise in the energy sector.



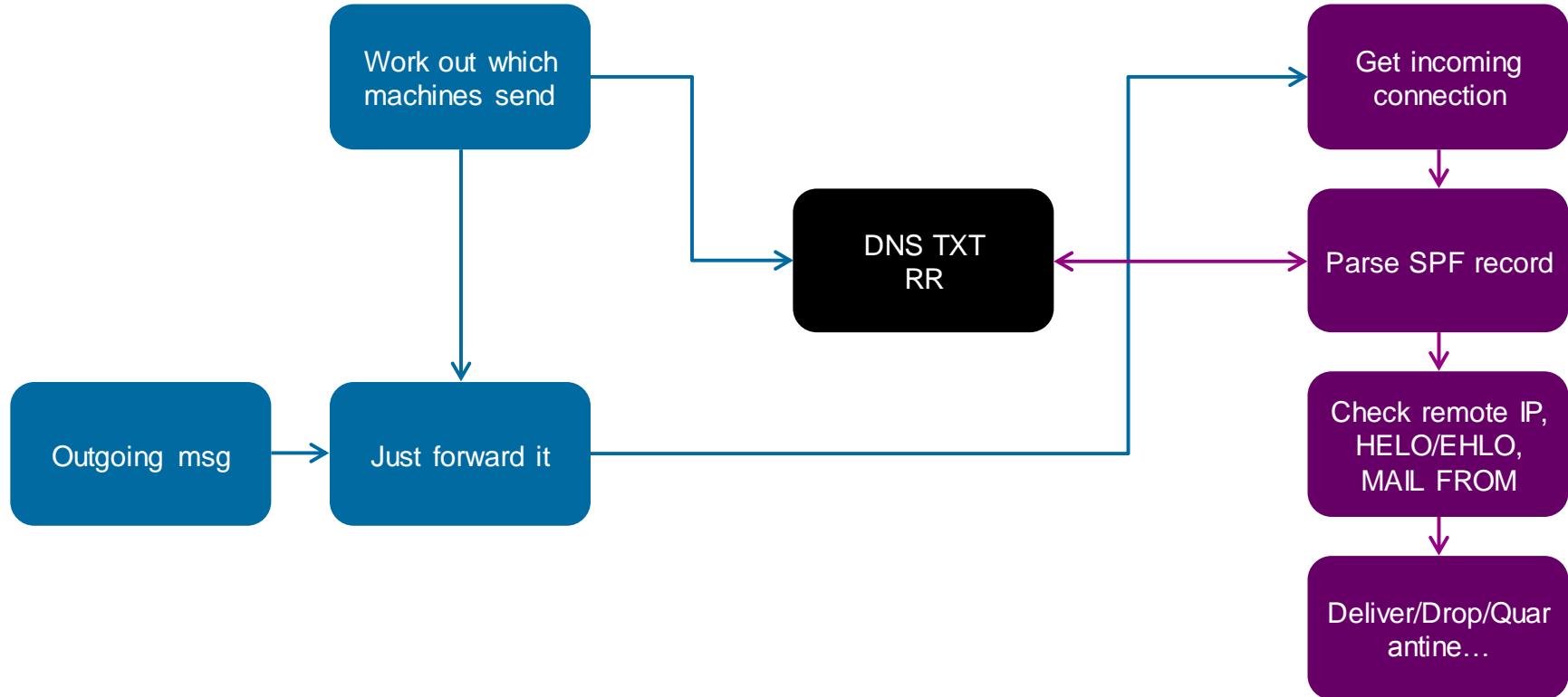
Securing your E-mail Infrastructure: SPF

Sender Policy Framework

A Short Introduction

- Specified in RFC7208, obsoletes RFC4408(bis) as of April 2014
- In a nutshell: Allows recipients to verify sender IP addresses by looking up DNS records listing authorised Mail Gateways for a particular domain
- Uses DNS TXT(16) (previously also SPF (Type 99)) Resource Records
 - SPF RR was obsoleted in RFC7208 due to low use and potential confusion
- Can verify HELO and MAIL FROM identity (FQDN)

SPF Operation



SPF Record Semantics

Found v=spf1 record for cisco.com:

SPF version

v=spf1 ip4:173.37.147.224/27 ip4:173.37.142.64/26
ip4:173.38.212.128/27 ~all

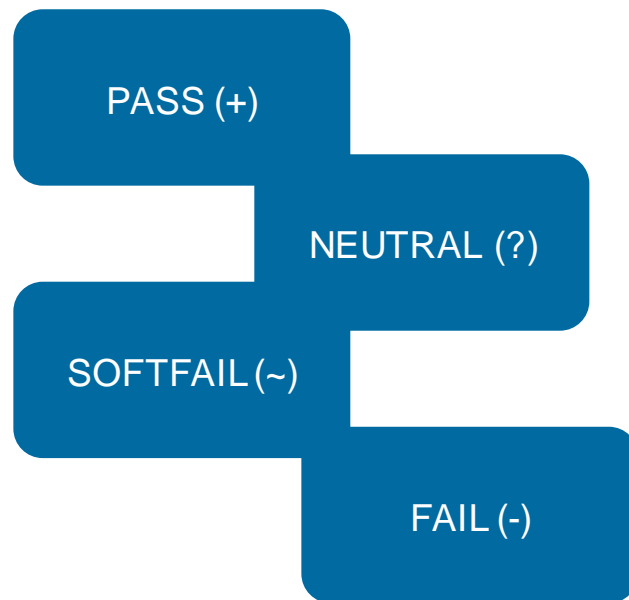
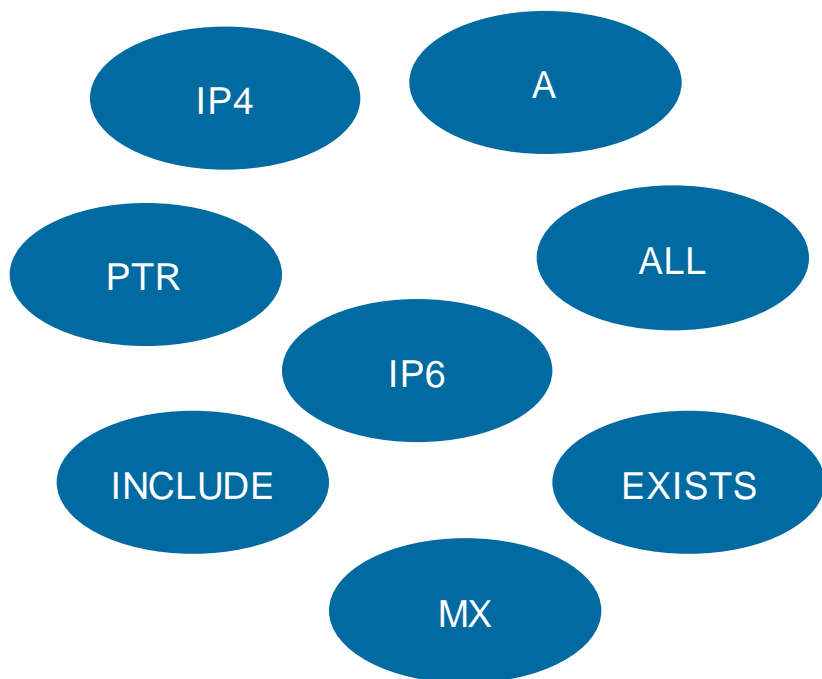
Verification

mechanisms

SPF Tool: <http://www.kitterman.com/spf/validate.html>

SPF Record Semantics

Mechanisms and Qualifiers



SPF Record Examples

```
cisco.com IN TXT "v=spf1 ip4:173.37.147.224/27  
ip4:173.37.142.64/26 ip4:173.38.212.128/27 ip4:173.38.203.0/24  
ip4:64.100.0.0/14 ip4:72.163.7.160/27 ip4:72.163.197.0/24  
ip4:144.254.0.0/16 ip4:66.187.208.0/20 ip4:173.37.86.0/24" "  
ip4:64.104.206.0/24 ip4:64.104.15.96/27 ip4:64.102.19.192/26  
ip4:144.254.15.96/27 ip4:173.36.137.128/26 ip4:173.36.130.0/24  
mx:res.cisco.com ~all"
```

```
amazon.com IN TXT "v=spf1 include:spf1.amazon.com  
include:spf2.amazon.com include:amazonses.com -all"
```

```
amazon.ses.com IN TXT "v=spf1 ip4:199.255.192.0/22  
ip4:199.127.232.0/22 ip4:54.240.0.0/18 ~all"
```

```
openspf.org IN TXT "v=spf1 -all"
```

SPF Record Nesting

```
google.com IN TXT "v=spf1 include:_spf.google.com ip4:216.73.93.70/31  
ip4:216.73.93.72/31 ~all"
```

```
_spf.google.com IN TXT "v=spf1 include:_netblocks.google.com  
include:_netblocks2.google.com include:_netblocks3.google.com ~all"
```

```
_netblocks.google.com IN TXT "v=spf1 ip4:216.239.32.0/19 ip4:64.233.160.0/19  
ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:209.85.128.0/17 ip4:66.102.0.0/20  
ip4:74.125.0.0/16 ip4:64.18.0.0/20 ip4:207.126.144.0/20 ip4:173.194.0.0/16 ~all"
```

```
_netblocks2.google.com IN TXT "v=spf1 ip6:2001:4860:4000::/36  
ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36  
ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all"
```

```
_netblocks3.google.com IN TXT "v=spf1 ~all"
```

- Maximum of 10 mechanisms querying DNS (any other than IP4, IP6, ALL)!

What SPF Does NOT Address

- Primary purpose of SPF is to validate whether a message sender comes from a legitimate host
- Only checks Envelope From – headers can still be faked
 - Complementary technology, SenderID, checks purported sender (“Purported Responsible Address”) in the headers, but has many shortcomings
- Does not ensure message integrity
- Does not prevent intra-domain forgery

SPF Best Practices

- Plan to include “-a11” in your SPF records
 - Consider all legitimate servers sending e-mail on your behalf
 - Make it part of security policy for roaming users to use authenticated SMTP on your gateways for sending outgoing mail
- Add your relay hosts’ HELO/EHLO identity to SPF records
- Create SPF records for all of your subdomains too
 - Publish null SPF records for domains/hosts that don’t send mail!
`nomail.domain.com. IN TXT "v=spf1 -a11"`
- Only include “MX” mechanism if your **incoming** mail servers also **send outgoing** mail



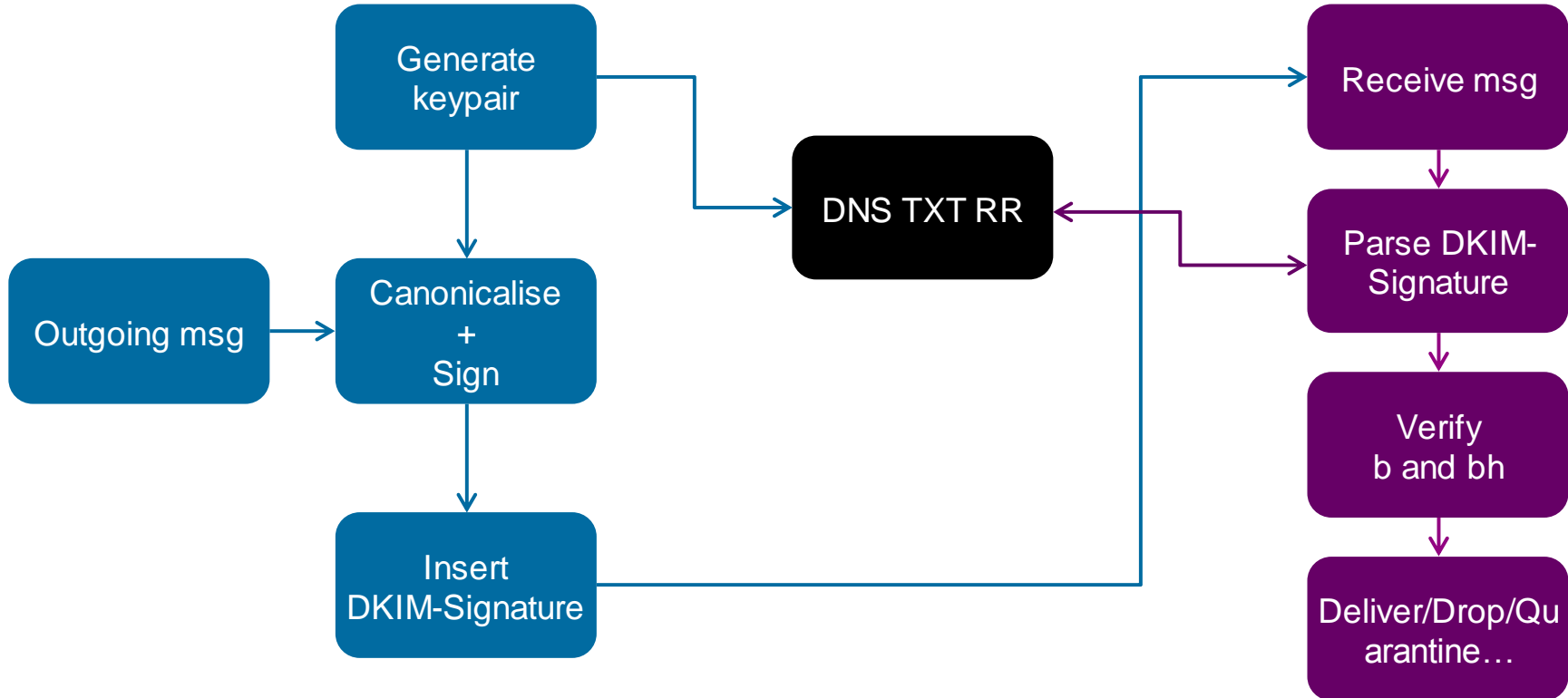
Securing Your E-mail Infrastructure: DKIM

Domain Keys Identified Mail

A Short Introduction

- Specified in RFC5585
 - Additional RFCs: RFC6376 (DKIM Signatures), RFC5863 (DKIM Development, Deployment and Operation), RFC5617 (Author Domain Signing Practices (ADSP))
- In a nutshell: Specifies methods for gateway-based cryptographic signing of outgoing messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages
- Uses DNS TXT records to publish public keys

DKIM Operation



DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalisation scheme

Signing Domain ID

Selector

Signed Headers

Header Hash

Body Hash

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=gmail.com; s=20120113;  
h=mime-version:date:message-id:subject:from:to:content-type;  
bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+AD1VSR6I0zrYofA=;  
b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhdWk9Yp0k8DuU4zgLh  
srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B  
JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh  
Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq  
ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ  
SyGhUFeuqwxJoCJcghGf7edZ00IgzTEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Signature

Algorithms

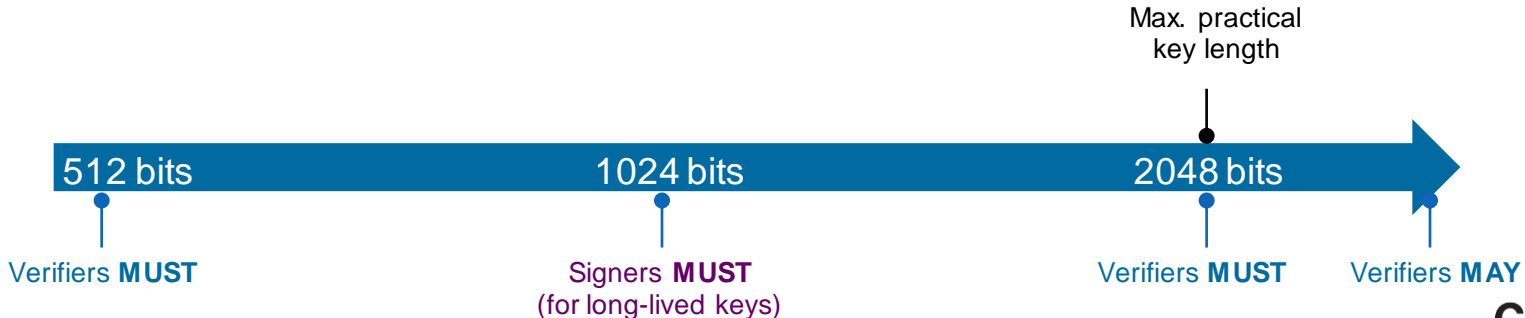
RSA-SHA1 or RSA-SHA256



Signers **MUST**
Verifiers **MUST**



Signers **SHOULD**
Verifiers **MUST**



DKIM Signature

Canonicalisation

- Process of adapting the message content for signing to compensate for minor changes by MTAs in transit
- **MUST NOT** change the transmitted data in any way; just its presentation
- Two canonicalisation schemes are supported for both headers and body:
 - Simple (almost no modification tolerated)
 - Relaxed (some modification, like header name case changes, line wrapping, whitespace replacement allowed)

DKIM Signature

Header Canonicalisation

- Simple Header Canonicalisation
 - No changes to headers
 - Retains order, case and whitespacing
- Relaxed Header Canonicalisation
 - Header names -> lowercase
 - Unfolds all multiline headers
 - Replaces sequences of WSP characters with a single WSP
 - Deletes WSP characters at EOL
 - Deletes WSP before and after the colon separating the field name from the value

DKIM Signature

Header Canonicalisation in Action

```
Return-Path: v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
X-Original-To: joemontes@montes.com.au
Delivered-To: joemontes@montes.com.au
Received: from mx1.hc4-93.c3s2.smtpi.com (esa1.hc4-93.c3s2.smtpi.com [68.232.136.98])
    by rotkvica.montes.com.au (Postfix) with ESMTP id B08562ABC01E
    for <joemontes@montes.com.au>; Thu, 26 Dec 2013 12:03:32 +0100 (CET) Received-SPF: Pass (mx1.hc4-
93.c3s2.smtpi.com: domain of
    v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
    designates 208.95.132.58 as permitted sender)
    identity=mailfrom; client-ip=208.95.132.58;
    receiver=mx1.hc4-93.c3s2.smtpi.com;
    envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
    x-sender=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
    x-conformance=sidf_compatible; x-record-type="v=spf1"
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
    postmaster@mail2112.eckler.mkt1970.com designates
    208.95.132.58 as permitted sender) identity=helo;
    client-ip=208.95.132.58; receiver=mx1.hc4-93.c3s2.smtpi.com;
    envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com;
    x-sender="postmaster@mail2112.eckler.mkt1970.com";
    x-conformance=sidf_compatible; x-record-type="v=spf1"
Authentication-Results: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (signature verified)
header.i=email@ecklers.messages1.com
X-IronPort-Anti-Spam-Filtered: true
```

DKIM Signature

Header Canonicalisation in Action

```
return-path:v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com
x-original-to:joemontes@montes.com.au
delivered-to:joemontes@montes.com.au
received:from mx1.hc4-93.c3s2.smtpi.com (esa1.hc4-93.c3s2.smtpi.com [68.232.136.98]) by
rotkvica.montes.com.au (Postfix) with ESMTP id B08562ABC01E for <joemontes@montes.com.au>; Thu, 26 Dec 2013
12:03:32 +0100 (CET)
received-spf:Pass (mx1.hc4-93.c3s2.smtpi.com: domain of v-
hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com designates 208.95.132.58 as permitted sender)
identity=mailfrom; client-ip=208.95.132.58; receiver=mx1.hc4-93.c3s2.smtpi.com; envelope-from=v-
hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-sender=v-
hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-conformance=sidf_compatible; x-record-type="v=spf1"
received-spf:Pass (mx1.hc4-93.c3s2.smtpi.com: domain of postmaster@mail2112.eckler.mkt1970.com designates
208.95.132.58 as permitted sender) identity=helo; client-ip=208.95.132.58; receiver=mx1.hc4-
93.c3s2.smtpi.com; envelope-from=v-hcjblh_lhnfmmhee_lcnjocf_lcnjocf_a@bounce.mkt1970.com; x-
sender=postmaster@mail2112.eckler.mkt1970.com; x-conformance=sidf_compatible; x-record-type="v=spf1"
authentication-results:mx1.hc4-93.c3s2.smtpi.com; dkim=pass (signature verified)
header.i=email@ecklers.messages1.com
x-ironport-anti-spam-filtered:true
```

DKIM Signature

Body Canonicalisation

- Simple Body Canonicalisation
 - No changes to the message, except:
 - removes any empty lines at the end of the message body
 - adds CRLF at the end of the message body, if not already there
- Relaxed Body Canonicalisation
 - Simple Canonicalisation, plus:
 - Ignores all WSP characters at EOL
 - Replaces sequences of WSP characters in a line into a single WSP

DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalisation scheme

Signing Domain ID

Selector

Signed Headers

Header Hash

Body Hash

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=gmail.com; s=20120113;  
h=mime-version:date:message-id:subject:from:to:content-type;  
bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+AD1VSR6I0zrYofA=;  
b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhdWk9Yp0k8DuU4zgLh  
srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B  
JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh  
Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq  
ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ  
SyGhUFeuqwxJoCJcghGf7edZ00IgzTEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Signature

Signing Domain ID and Selector

- Signing Domain ID (SDID)
 - Identifies the entity claiming responsibility for the signed message
 - Must correspond to a valid DNS name under which a DKIM key is published
- Selector
 - Enables publishing of multiple keys per signing domain
 - Use cases:
 - Periodic key rotations
 - Delegating/splitting signing authority for different OUs
 - Delegating signing authority to 3rd parties
 - Allowing roaming users to sign their own messages

DKIM Signature

Example DKIM-Signature Header

Algorithms used

Canonicalisation scheme

Signing Domain ID

Selector

Signed Headers

Header Hash

Body Hash

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=gmail.com; s=20120113;  
h=mime-version:date:message-id:subject:from:to:content-type;  
bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+AD1VSR6I0zrYofA=;  
b=n3EBxT5DwNbeISSYpKT6zOKHEb8ju51F4X8H2BKhdWk9Yp0k8DuU4zgLh  
srfeFCvf+/2XEPnQaIVtKmE0h7ZTI8yvV6lDEQtJQQWqQ/RA7WsN4Tjg4B  
JAXPR+yF6xwLLcQqMwzsgLxC3pQAPw3Lp7py9C62nauei3nLEm0gLnXYsh  
Uvq6IS+qfJBOKeMby9WUsqRecg0AWX8Dfb8gxXHQH8wKFJ96KitB6iPFq  
ufIOTaZWMhiFnL+NHR06v0PwsCQhsSccuk0eTDu9Uqyf8bDn4opkhg7tZ  
SyGhUFeuqwxJoCJcghGf7edZ00IgzTEcuxLMcgl+mpSje2YIfeXgFRg==
```

DKIM Public Key Retrieval

- DNS query:

<selector>._domainkey.<SDID>

- For our example:

```
20120113._domainkey.gmail.com IN TXT "k=rsa\;  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabg  
bFwh+eBCsSTRqmwIYYvywlbhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyo  
xcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD0" "7y2+07w1NWwIt  
8svnxgdxGkVbbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIh  
kx4xYSIc9oSvmAl50ctMEeWUwg8Istjqz8BZeTWbf41fbNhte7Y+YqZ0wq1S  
d0DbvYAD9NOZK9vlfuac0598HY+vtSBczUiKERHv1yRbcaQtZFh5wtiRrN04B  
LUTD21MycBX5jYchHjPY/wIDAQAB"
```


DKIM Signature

Anatomy of the DKIM-Signature Header

Mandatory tags

V	A	D	S	H	B	BH
---	---	---	---	---	---	----

Optional tags

C	I	L	Z
---	---	---	---

Recommended tags

T	X
---	---

DKIM Signature Tags

Expanded View

- Required signature tags:
 - v, a, d, s, h, b, bh
- Optional signature tags:
 - c – defaults to simple/simple
 - i – Agent or User ID – usually corresponds to sender's e-mail address
 - l – Body length
 - z – Copied header fields, separated by “|” – used for diagnostics
- Recommended signature tags:
 - t – Signature timestamp in Unix Epoch time, GMT
 - x – Signature expiration in Unix Epoch time, GMT. Must be greater than “t” time

DKIM Public Key

Anatomy of the DKIM DNS Record

Mandatory tags

P

Optional tags

H=SHA1 K=RSA S=EMAIL T=Y T=S G N

Recommended tags

V=DKIM1

DKIM Public Key

Expanded Tags

- Only “p” tag is required
- Optional tags:
 - h – acceptable hash algorithms
 - k – key type
 - n – notes (for human interpretation)
 - s – service type
 - g – key granularity; local part of the “i” tag of the signature must be equal to it
 - t – flags
 - y – This domain is testing DKIM
 - s – if “i” tag is used in signature, domain part of the “i” tag must be equal to “d” tag. Recommended to be present if no subdomains are used.
- Recommended tags:
 - v – Version of the DKIM key record. If present, must be “DKIM1”.

DKIM Public Key Examples

```
iport._domainkey.cisco.com IN TXT "v=DKIM1\; s=email\;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCctxGhJnvNpdcQLJM6a/0otvd  
pzFIJuo73OYFuw6/8bXcf8/p5JG/iME1r9fUl rNZs3kMn9ZdPYvTyRbyZ0  
UyMrsM3ZN2JAIop3M7sitqHgp8pbORFgQyZxq+L23I2cELq+qwtbanjWJzEPpV  
vrvbuz9QL8CUTS+V5N51dq8L/lwIDAQAB\;"
```

```
lufthansa3._domainkey.lufthansa.com IN TXT "g=*\; k=rsa\; t=y\;  
n="Contact postmaster@responsys.com with any questions concerning  
this signing"\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA7e  
WF9kW/HY6ppS6g3U6Be0JRfu59Iv3oYgW+ztdJK1HsLf/hmah4buPBtVaGb  
CagDNN7wK12uhs6ko6f4Su1ZpwqVdtp1R6jujvW56hcNhx4RJ0E17mefniciwYfQx  
DhQmE81kUzJR4BXWuKsPSSSy/pT3rM+LusuTAbFWKsMQIDAQAB\;"
```

Choosing Your DKIM Parameters

- Make the best use of selectors
 - Periodic key rotation
 - Delegation of signing authority
 - Sacrificing security for performance
 - If you must, consider “weakening” your signatures in the following order:
 - Reduce the signing key size (and combine with selector rotation)
 - Use “simple” for body canonicalisation
 - Use “simple” for headers canonicalisation
 - Change signing algorithm to sha-1
- However, RFC6376 says: “Signers MUST implement and SHOULD sign using rsa-sha256”

A nighttime city street scene with a pedestrian bridge and light trails from traffic. The scene is illuminated by city lights and traffic signals, creating a vibrant urban atmosphere. The light trails are primarily yellow and orange, indicating long-exposure photography of moving vehicles. The pedestrian bridge is a prominent feature in the middle ground, with its structure and lights clearly visible. In the background, several high-rise buildings are lit up, adding to the city's skyline. The overall composition is dynamic and modern.

Securing Your E-mail Infrastructure: DMARC

“DMARC is designed to prevent bad mailers from sending mail which claims to come from legitimate senders, particularly senders of transactional email.

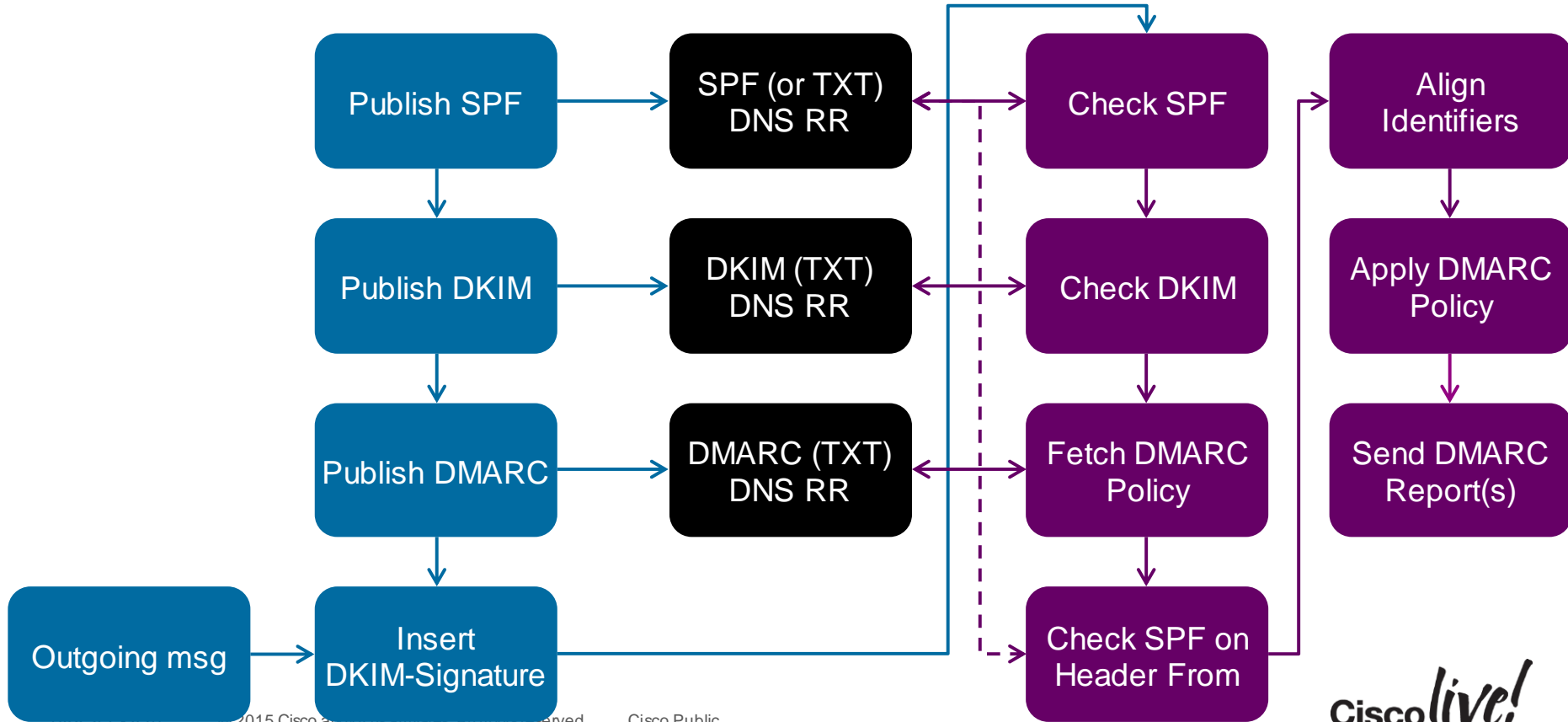
One of the primary uses of this kind of spoofed mail is phishing”

- [draft-kucherawy-dmarc-base-04](#)
- IETF Network Working Group

Moving Towards DMARC

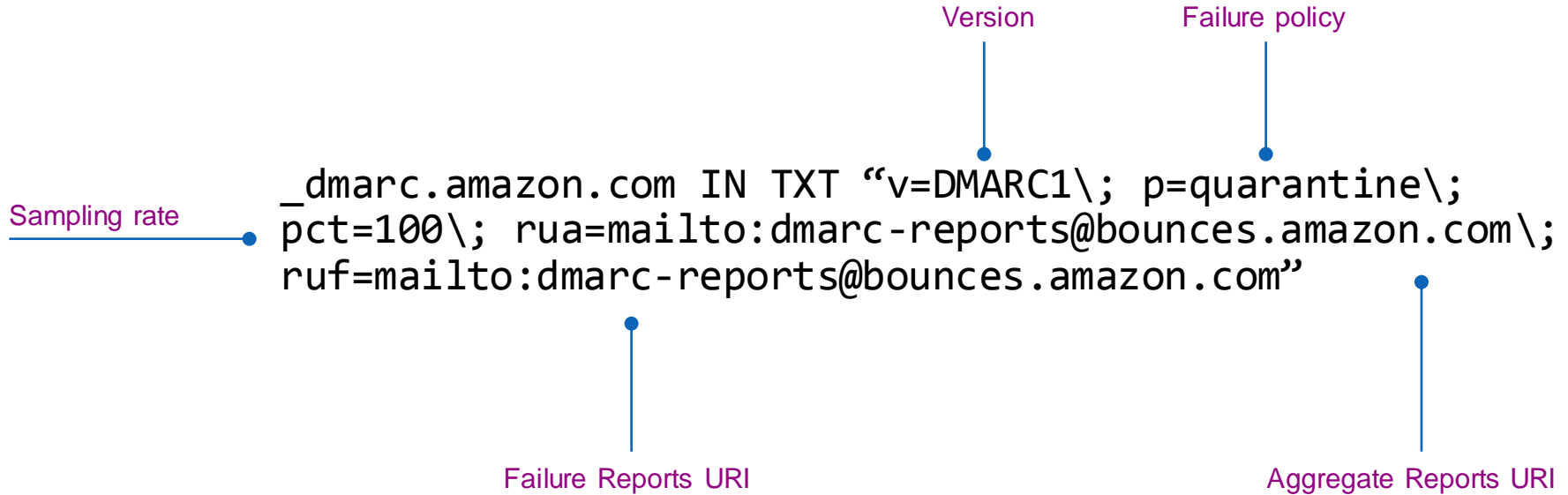
- Both DKIM and SPF have shortcomings, not because of bad design, but because of different nature of each technology
- DKIM policy advertising was addressed by ADSP, but:
 - There was no visibility by spoofed parties into offending traffic
 - Even though a receiver implemented both SPF and DKIM verification, there was no requirement of the two technologies being in sync
 - A smart attacker might make use of this to push illegitimate messages through
- SPF checks HELO/MAILFROM identity, but no verification or alignment of Header From is ensured
- Thus, DMARC was born:
 - Leveraging great existing technologies, providing a glue to keep them in sync, and allowing **senders** to mandate rejection policies and have visibility of offending traffic

DMARC Operation



DMARC Policy

Example of a DMARC DNS Record



DMARC Policy

Policy Specification and “Slow Start”

- Policies requested by senders:
 - None
 - Quarantine
 - Reject
- Receivers MAY deviate from requested policies, but SHOULD inform the sender why (through Aggregate Report)
- Sampling rate (“p” tag) instructs the receiver to only apply policy to a fraction of messages

DMARC Policy

Reporting URIs

- mailto: and http:// URIs supported
- Two distinct report types:
 - Aggregate report
 - Sent on an interval
 - Summary of all incidents from a particular sender domain
 - Failure report
 - Sent on (every) failure
 - Detailed report on individual failures

DMARC Policy

Anatomy of the DMARC DNS Record

Mandatory tags

V=DMARC1	P
----------	---

Optional tags

PCT	SP	ADKIM	ASPF	RI	RUA	RF	FO	RUF
-----	----	-------	------	----	-----	----	----	-----

DMARC Policy

Adherence to SPF/DKIM

- Sender can request Strict (“s”) or Relaxed (“r”, default) adherence to DKIM and SPF
- DKIM (“adkim”):
 - Relaxed: Header From FQDN can be a subdomain of “d” tag of DKIM signature
 - Strict: Header From FQDN must completely match the “d” tag of DKIM
- SPF (“aspf”):
 - Relaxed: Header From domain can be a subdomain of SPF-Authenticated (MAIL FROM) domain
 - Strict: Header From domain must match MAIL FROM domain

DMARC Policy

Failure Reporting

- Two supported Report Formats (“rf”):
 - afrf
 - Authentication Failure Reporting Format, defined in RFC6591, and extended by draft-kucherawy-dmarc-base (default)
 - iodef
 - Incident Object Description Exchange Format, defined in RFC5070
- Failure reporting options (“fo”), separated by colons in the Policy Record:
 - 0 : generate a report if **all** underlying mechanisms fail to align and pass (default)
 - 1 : generate a report if **any** underlying mechanisms fail to align and pass
 - d : generate a DKIM failure report if DKIM verification fails, regardless of alignment
 - s : generate an SPF failure report for failed SPF verification, regardless of alignment

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;  
ruf=mailto:d@ruf.agari.com\;"
```

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;  
ruf=mailto:d@ruf.agari.com\";
```

ruf.agari.com

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;  
ruf=mailto:d@ruf.agari.com\";
```

facebook.com

ruf.agari.com

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;  
ruf=mailto:d@ruf.agari.com\";
```

facebook.com._report._dmarc.ruf.agari.com

DMARC Reporting

Delegating Reporting Authority

```
_dmarc.facebook.com IN TXT "v=DMARC1\; p=reject\; pct=100\;  
rua=mailto:d@rua.agari.com,mailto:postmaster@facebook.com\;  
ruf=mailto:d@ruf.agari.com\";
```

```
facebook.com._report._dmarc.ruf.agari.com IN TXT "v=DMARC1"
```

DMARC Record Examples

_dmarc.google.com IN TXT “v=DMARC1\; p=quarantine\; rua=mailto:mailauth-reports@google.com”

_dmarc.cs.helsinki.fi IN TXT “v=DMARC1\; p=reject\; sp=reject\; pct=100\; aspf=r\; rua=mailto:dmarc-reports@cs.helsinki.fi”

_dmarc.microsoft.com IN TXT “v=DMARC1\; p=none\; pct=100\; rua=mailto:d@rua.agari.com\; ruf=mailto:d@ruf.agari.com\; fo=1”

_dmarc.dk-hostmaster.dk IN TXT “v=DMARC1\; p=none\; rua=mailto:dmarc-report@dk-hostmaster.dk\; ruf=mailto:dmarc-report@dk-hostmaster.dk\; adkim=r\; aspf=r\; rf=afrrf”

DMARC Identifier Alignment

When Does A Message Pass?

- DMARC authenticates the domain from Header From
- DKIM authenticates the domain from DKIM-Signature (“d” tag)
- SPF authenticates domains from MAIL FROM or HELO identities
- **Identifier Alignment** is a concept of alignment between Header From and identifiers checked by DKIM and SPF
- Message **passes** DMARC check if **one or more** of the authentication mechanisms (DKIM **and/or** SPF) pass **with proper alignment**

DMARC Policy

Anatomy of the DMARC DNS Record

Mandatory tags

V=DMARC1	P
----------	---

Optional tags

PCT	SP	ADKIM	ASPF	RI	RUA	RF	FO	RUF
-----	----	-------	------	----	-----	----	----	-----

DMARC Policy

Adherence to SPF/DKIM

- Sender can request Strict (“s”) or Relaxed (“r”, default) adherence to DKIM and SPF
- DKIM (“adkim”):
 - Relaxed: Header From FQDN can be a subdomain of “d” tag of DKIM signature
 - Strict: Header From FQDN must completely match the “d” tag of DKIM
- SPF (“aspf”):
 - Relaxed: Header From domain can be a subdomain of SPF-Authenticated (MAIL FROM) domain
 - Strict: Header From domain must match MAIL FROM domain

DMARC Identifier Alignment: SPF

MAIL FROM: <joemonte@cisco.com>

From: Joe Montes (joemonte) <joemonte@cisco.com>

To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

DMARC Identifier Alignment: SPF

MAIL FROM: <joemonte@cisco.com>

From: Joe Montes (joemonte) <joemonte@cisco.com>

To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

DMARC Identifier Alignment: SPF

aspf="r" aspf="s"

MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

DMARC Identifier Alignment: SPF

aspf="r" aspf="s"

MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

MAIL FROM: <joemonte@cisco.com>

From: Joe Montes (joemonte) <joemonte@mail.cisco.com>

To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

DMARC Identifier Alignment: SPF

aspf="r" aspf="s"

MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test



MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@mail.cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test



DMARC Identifier Alignment: SPF

aspf="r" aspf="s"

MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test



MAIL FROM: <joemonte@cisco.com>



From: Joe Montes (joemonte) <joemonte@mail.cisco.com>



To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test



MAIL FROM: <joemontes@montes.com.au>

From: Joe Montes (joemonte) <joemonte@cisco.com>

To: Joe Montes <joemontes@montes.com.au>

Subject: DMARC test

DMARC Identifier Alignment: SPF

aspf="r" aspf="s"

MAIL FROM: <joemonte@cisco.com>

From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



MAIL FROM: <joemonte@cisco.com>

From: Joe Montes (joemonte) <joemonte@mail.cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



MAIL FROM: <joemontes@montes.com.au>

From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



DMARC Identifier Alignment: DKIM

```
DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test
```

DMARC Identifier Alignment: DKIM

DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



adkim="r"



adkim="s"



DMARC Identifier Alignment: DKIM

DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test

adkim="r"

adkim="s"



DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@mail.cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test

DMARC Identifier Alignment: DKIM

DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



adkim="r"




adkim="s"



DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@mail.cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



DMARC Identifier Alignment: DKIM


DKIM-Signature: v=1; [...] d=cisco.com; [...] 
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test

adkim="r"



adkim="s"



DKIM-Signature: v=1; [...] d=cisco.com; [...] 
From: Joe Montes (joemonte) <joemonte@mail.cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



DKIM-Signature: v=1; [...] d=montes.com.au; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test

DMARC Identifier Alignment: DKIM

DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test

adkim="r"

adkim="s"



DKIM-Signature: v=1; [...] d=cisco.com; [...]
From: Joe Montes (joemonte) <joemonte@mail.cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



DKIM-Signature: v=1; [...] d=montes.com.au; [...]
From: Joe Montes (joemonte) <joemonte@cisco.com>
To: Joe Montes <joemontes@montes.com.au>
Subject: DMARC test



DMARC

How to start

1. Correctly deploy DKIM and SPF
2. Make sure that your identifiers will align
3. Publish a DMARC record with “p=none”, gather rua and ruf reports for a while
4. Analyse the data and modify your mail streams (or DKIM/SPF parameters)
5. Apply “reject” or “quarantine” policy

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-conformance=sidf_compatible; x-record-type="v=spf1"
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
+c8vp3q89JcMLPtRf010tRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
Q/gNPFkJJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```


DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure `adkim` is set to `strict`, and `aspf` set to `relaxed` if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTP; 01
Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-conformance=sidf_compatible; x-record-type="v=spf1"
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
+c8vp3q89JcMLPtRf010tRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiiZPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
Q/gNPFkJJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure adkim is set to strict, and aspf set to relaxed if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTMP; 01
Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-conformance=sidf_compatible; x-record-type="v=spf1"
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
+c8vp3q89JcMLPtRf010tRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiizPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
Q/gNPFkJJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```

DMARC

How to Delegate

- Create a subdomain for your 3rd party mailers
- Provide them with your DKIM signing key
- Make sure adkim is set to strict, and aspf set to relaxed if needed

```
Received: from mta3.e.tripadvisor.com ([66.231.81.9]) by mx1.hc4-93.c3s2.smtpi.com with ESMTMP; 01
Jan 2014 21:16:36 +0100
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: domain of
bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com designates 66.231.81.9
as permitted sender) identity=mailfrom; client-ip=66.231.81.9; receiver=mx1.hc4-93.c3s2.smtpi.com;
envelope-from="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-sender="bounce-891195_HTML-783170676-35558060-77825-258@bounce.e.tripadvisor.com";
x-conformance=sidf_compatible; x-record-type="v=spf1"
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=200608; d=e.tripadvisor.com;
h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:Message-ID:Content-Type;
i=members@e.tripadvisor.com; bh=ZNcj7Ir0D/Hc0M9uybYZydUdcZQ=; b=afqcdGZ2Vg8z38JBi8xKU
+c8vp3q89JcMLPtRf010tRV21UjsQgW1fKCFBZglZxnyQuE8TLGQJy2AkaCaV2YiizPogw6PhNmmDMmxG2i5ufgqvipfZezvTu
Q/gNPFkJJeUFSHRpJriV0017gsGVmV3t72fv25kS0kKbtvvhjZCyQ=
From: "TripAdvisor" <members@e.tripadvisor.com>
```



Enhanced Security Features

URL Filtering

- Checks for reputation and category of URL's in messages (in/out)
- Used now in Anti-Spam and Outbreak filters
- URL Actions
 - Block based on category
 - Rewrite (send to Infosec Web site)
 - Defang (BLOCKEDwww.ihaveabadreputation.comBLOCKED)
 - Replace URL with a TEXT Message

URL Filtering



Cisco C000V
Email Security Virtual Appliance



Monitor

Mail Policies

Security Services

Network

System Administration

URL Filtering

URL Filtering Overview

URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Whitelist:	None

[Edit Global Settings...](#)

Copyright © 2003-2014 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

URL Filtering

The screenshot displays the Cisco C000V Email Security Virtual Appliance interface. The main window is titled 'Edit Content Filter' and shows settings for a filter named 'URL...'. The 'Conditions' section contains one condition: 'URL Category'. The 'Actions' section contains one action: 'URL Reputation'. An 'Edit Condition' dialog is open, showing a list of conditions with 'URL Category' selected. The dialog also shows a list of available categories and a list of selected categories.

Edit Condition

Message Body or Attachment
Message Body
URL Category
URL Reputation
Message Size
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
DKIM Authentication
SPF Verification

URL Category Help

Does any URL in the message body or subject belong to one of the selected categories?

Available Categories:

- Adult
- Advertisements
- Alcohol
- Arts
- Astrology
- Auctions
- Business and Industry
- Chat and Instant Messag
- Cheating and Plagiarism
- Computer Security
- Computers and Internet
- Dating
- Digital Postcards
- Dining and Drinking
- Dynamic and Residentia

Selected Categories:

- Child Abuse Content
- Filter Avoidance
- Gambling
- Hate Speech
- Illegal Downloads
- Parked Domains
- Peer File Transfer
- Pornography
- Software Updates

Use a URL whitelist: ?

Cancel OK

URL Filtering

The screenshot displays the Cisco C000V Email Security Virtual Appliance interface. The main window is titled "Edit Content Filter" and is divided into three sections: "Content Filter Settings", "Conditions", and "Actions".

Content Filter Settings:

- Name: URL
- Currently Used by Policies: Default
- Description: (empty)

Conditions:

Order	Condition
1	URL Category

Actions:

Order	Action
1	URL Reputation

Edit Action Dialog:

URL Reputation Help

What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (WBRS).

URL Reputation is:

- Malicious (-10.0 to -6.0)
- Suspect (-5.9 to 5.9)
- Clean (6.0 to 10.0)
- Custom Range (min to max)
[] []
- No Score

Use a URL whitelist: ?

Action on URL:

- Defang URL ?
- Redirect to Cisco Security Proxy ?
- Replace URL with text message

Perform Action for:

- All messages
- Unsigned messages

Other actions listed in the dialog include: Quarantine, Encrypt on Delivery, Strip Attachment by Content, Strip Attachment by File Info, Add Disclaimer Text, Bypass Outbreak Filter Scanning, Bypass DKIM Signing, Send Copy (Bcc:), Notify, Change Recipient to, Send to Alternate Destination Host, Deliver from IP Interface, Strip Header, Add/Edit Header, Add Message Tag, Add Log Entry, Encrypt and Deliver Now (Final Action), Bounce (Final Action), Skip Remaining Content Filters (Final Action), and Drop (Final Action).

AMP – Advanced Malware Protection

- Checks file threats based
 - File reputation
 - File sandboxing (unknown reputation)
 - Retrospective verdicts
 - Only sends the SHA256 Hash value of the file

File Reputation and Analysis

Advanced Malware Protection

File Reputation:	Enabled
File Analysis:	Enabled

[Edit Global Settings...](#)

Incoming Mail Policies

Find Policies

Email Address:

Recipient
 Sender

Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop	URL_Filter	Retention Time: Virus: 1 day	

Key: Default Custom Disabled

Mail Policies: Advanced Malware Protection

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="checkbox"/> Enable File Analysis <input type="radio"/> No
Message Scanning	
	<input type="checkbox"/> (recommended) Include an X-header with the AMP results in messages
Unscannable Attachments:	
Action Applied to Message:	Deliver As Is <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: ATTACHMENT UNSCANNE
▸ Advanced	Add Custom Header to Message: <input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Messages with Malware Attachments:	
Action Applied to Message:	Drop Message <input type="button" value="v"/>
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: MALWARE DETECTED]
▸ Advanced	Optional settings for custom header.

Outbreak Filters

Introduced in AsyncOS 7.5.x



Delay

- Suspicious Threat Msgs
- All Threat Types (spam, phishing, targeted)



Redirect

- Suspect URLs via Cisco Cloud Web Security



Modify

- Message Content (subject line)
- Add Warning Statements

Outbreak Filters

Outbreak Filters Overview	
Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	512K
Receive Emailed Alerts:	No
Edit Global Settings...	

Outbreak Filter Rules		
Rule Updates		
Rule Type	Last Update	Current Version
CASE Core Files	15 Feb 2015 13:12 (GMT +00:00)	3.4.0-013
CASE Utilities	15 Feb 2015 13:12 (GMT +00:00)	3.4.0-013
Outbreak Rules	15 Feb 2015 13:12 (GMT +00:00)	20150215_115327
Outbreak Filter Rules (higher number indicates greater risk. 1= lowest threat, 5= highest threat)		
Above Quarantine Threshold		
Threat Level	Rule ID	Rule Description
3	OUTBREAK_0000188	System Test
3	OUTBREAK_0000189	System Test
3	OUTBREAK_0000190	System Test
3	OUTBREAK_0000858	We are seeing unusual volume for file extension(s) bat, cmd, exe, pif, scr, zip(bat), zip(cmd), zip(...
3	OUTBREAK_0000971	We are seeing unusual volume for file extension(s) bat, cmd, exe, pif, scr, zip(bat), zip(cmd), zip(...
3	OUTBREAK_0001123	We are seeing unusual volume for file extension(s) exe, scr, zip(exe), zip(scr), zip:e(exe), zip:e(s...
3	OUTBREAK_0001132	We are seeing unusual volume for file extension(s) exe, pif, scr, zip(exe), zip(pif), zip(scr), zip:...
3	OUTBREAK_0001160	We are seeing unusual volume for file extension(s) zip(hta), zip:e(hta). We are raising the Threat L...
3	OUTBREAK_0002969	We are seeing suspicious url(s) propagating through multiple sources. We are raising the Threat Leve...
3	OUTBREAK_0003900	We are seeing unusual volume for file extension(s) zip(exe), zip(scr), zip:e(exe), zip:e(scr). We

Mail Policies: Outbreak Filters

Outbreak Filtering for: Default Policy

Enable Outbreak Filtering (Customize settings) ▾

Outbreak Filter Settings

Quarantine Threat Level: ? ▾

Maximum Quarantine Retention: Days ▾

Other Threats: Hours ▾

Deliver messages without adding them to quarantine

Bypass Attachment Scanning: ▸ *None configured*

Message Modification

Enable message modification. Required for non-viral threat detection (excluding attachments)

Message Modification Threat Level: ? ▾

Message Subject:

Include the X-IronPort-Outbreak-Status headers:

- Enable for all messages
- Enable only for threat-based outbreak
- Disable

Include the X-IronPort-Outbreak-Description header:

- Enable
- Disable

Alternate Destination Mail Host (Other Threats only):

(examples: example.com, 10.0.0.1, 2001:420:80:1::5)

URL Rewriting: Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.

- Enable only for unsigned messages (recommended)
- Enable for all messages
- Disable

Bypass Domain Scanning ?

(examples: example.com, crm.example.com, 10.0.0.1, 10.0.0.0/24, 2001:420:80:1::5, 2001:db8::/32)

Threat Disclaimer: ▾

Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Tools > Resources > Disclaimers

S/MIME Support

- Available on AsyncOS 9.0
- Gateway S/MIME
 - Sign
 - Encrypt
 - Verify
 - Decrypt

Appliances

ESA – Email Security Appliance

Hardware

- C170
- C380
- C680

Virtual

- C000
- C100
- C300
- C600

SMA – Security Management Appliance

Hardware

- M170
- M380
- M680

Virtual

- M000
- M100
- M300
- M600

For More Information

- <http://www.openspf.org>
- <http://www.dkim.org>
- <http://blogs.cisco.com/security/big-data-in-security-part-v-anti-phishing-in-the-cloud/>
- <https://support.google.com/mail/answer/3070163?hl=en>
- <http://tools.ietf.org/html/draft-kucherawy-dmarc-base-04>
- <http://dmarc.org>
- <http://dmarcian.com>

Enhance Your Knowledge

- Demos in the Cisco World of Solutions
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings



Q & A

Cisco *live!*

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site
<http://showcase.genie-connect.com/clmelbourne2015>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

Cisco *live!*



CISCO